Claims

1. A method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, said method comprising:

encrypting the stream of data at said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit by changing at least one encryption parameter and signaling said change in encryption parameter to said decryption unit, said dynamically varying of said at least one encryption parameter being responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter.

2. The method of claim 1, wherein said at least one encryption parameter comprises at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

3. The method of claim 2, wherein said at least one encryption parameter comprises at least some of said encryption key, encryption granularity, encryption density scale, encryption density, encryption delay, encryption key update variable, and encryption key update data trigger.

4. The method of claim 2, further comprising multiplexing said changed encryption parameter and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameter and said encrypted data at said receiver.

5. The method of claim 1, wherein said dynamically varying comprises dynamically varying said encryption parameter based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

6. The method of claim 5, wherein said encryption parameter comprises an encryption key.

7. The method of claim 1, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

8. The method of claim 7, wherein said stream of compressed data can comprise one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

9. The method of claim 1, further comprising initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption parameter of said plurality of encryption parameters.

10. The method of claim 1, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed encryption parameter comprises one encryption parameter of said plurality of encryption parameters.

11. The method of claim 10, wherein said setting of said plurality of encryption parameters includes establishing at least some of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

12. The method of claim 1, wherein said encrypting comprises encrypting multiple portions of said data stream, and wherein said dynamically varying comprises dynamically varying said encrypting of said multiple portions of said data stream by changing said at least one encryption parameter for each portion of said multiple portions.

13. The method of claim 1, wherein said dynamically varying comprises dynamically varying said at least one encryption parameter responsive to passage of a predefined number of data bits in said stream of data, or alternatively, responsive to passage of a predefined number of data units in said stream of data, wherein said data units comprise at least one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

14. A system for protecting a stream of data comprising:

an encryption unit for encrypting the stream of data for transfer to a decryption unit;

means for dynamically varying said encrypting of said stream of data by said encryption unit by changing an encryption parameter and signaling said change in encryption parameter to said decryption unit, said means for dynamically varying being responsive to occurrence of a predefined condition in said stream of data; and

wherein said decryption unit decrypts said encrypted data, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter.

15. The system of claim 14, wherein said changed encryption parameter comprises an encryption key, and wherein said means for dynamically varying comprises a dynamic encryption key generator, and means for dynamically varying said encryption key based on an occurrence of a predefined condition in said stream of data.

16. The system of claim 15, wherein said stream of data comprises a stream of digital data.

17. The system of claim 14, wherein said means for dynamically varying comprises means for dynamically varying said encryption parameter based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

18. The system of claim 14, wherein said encryption unit encrypts multiple portions of the stream of data, and wherein said means for dynamically varying comprises means for changing said encryption parameter for each portion of said multiple portions of said stream of data.

19. The system of claim 14, wherein said at least one encryption parameter comprises at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

20. The system of claim 19, wherein said at least one encryption parameter comprises at least some of said encryption key, encryption granularity, encryption density scale, encryption density, encryption delay, encryption key update variable, and encryption key update data trigger.

21. The system of claim 14, further comprising a data multiplexer for multiplexing said changed encryption parameter into said encrypted data for transfer thereof to said decryption unit.

22. The system of claim 14, further comprising means for setting a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encryption unit and wherein said changed encryption parameter comprises one encryption parameter of said plurality of encryption parameters.

23. The system of claim 22, wherein said stream of data comprises a stream of compressed data, and wherein said system further comprises a decoder for decompressing said compressed data after decrypting thereof by said decryption unit.

24. The system of claim 23, wherein said stream of compressed data can comprise a stream of one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

25. The system of claim 22, wherein said means for setting said plurality of encryption parameters includes means for establishing at least some of an encryption granularity, an encryption key, a density scale, a density, an encryption delay, and a key update data trigger.

26. The system of claim 14, wherein said means for dynamically varying comprises means for changing said encryption parameter based on a predefined number of bits being encoded by said encryption unit, or alternatively, based on a predefined number of units being encoded by said encryption unit, said units comprising one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

27. A system for protecting a stream of data to be transferred between a sender and a receiver, said system comprising:

an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data by changing at least one encryption parameter based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameter to said receiver; and

a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed encryption parameter to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter.

28. At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, comprising;

encrypting the stream of data at said encryption unit for transfer thereof to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit by changing an encryption parameter and signaling said change in encryption parameter to said decryption unit, wherein

said dynamically varying of said encryption parameter is responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameter.

29. The at least one program storage device of claim 28, wherein said encryption parameter comprises at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

30. The at least one program storage device of claim 29, wherein said at least one encryption parameter comprises at least some of said encryption key, encryption granularity, encryption density scale, encryption density, encryption delay, encryption key update variable, and encryption key update data trigger.

31. The at least one program storage device of claim 29, wherein said method further comprises multiplexing said changed encryption parameter and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameter and said encrypted data at said receiver.

32. The at least one program storage device of claim 28, wherein said dynamically varying comprises dynamically varying said encryption parameter based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

33. The at least one program storage device of claim 32, wherein said encryption parameter comprises an encryption key.

34. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

35. The at least one program storage device of claim 34, wherein said stream of compressed data can comprise one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

36. The at least one program storage device of claim 28, wherein said method further comprises initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed encryption parameter of said dynamically varying comprises one encryption parameter of said

plurality of encryption parameters.

37. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed encryption parameter comprises one encryption parameter of said plurality of encryption parameters.

38. The at least one program storage device of claim 37, wherein said setting of said plurality of encryption parameters includes establishing at least some of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.